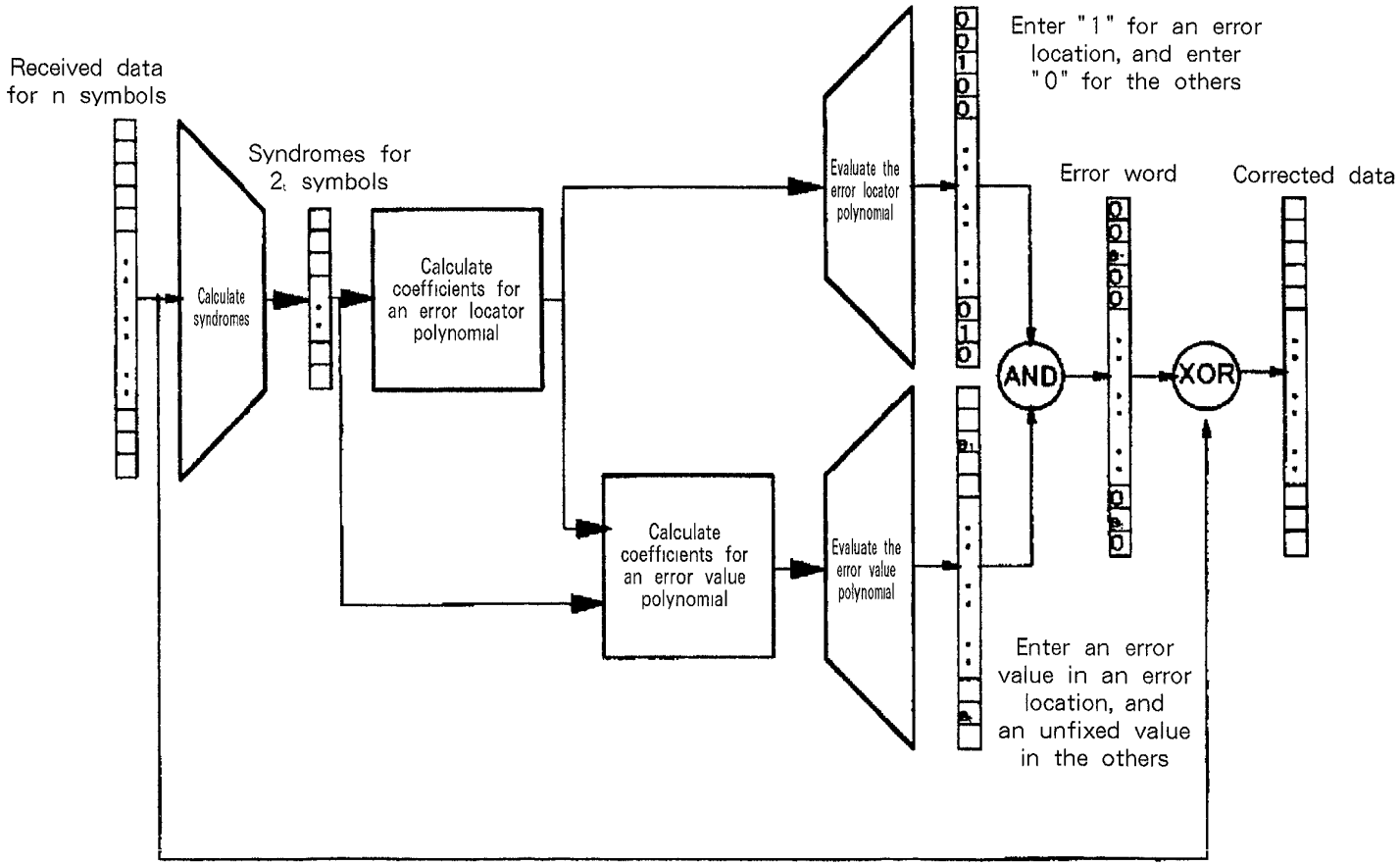


Fig. 1
PRIOR ART

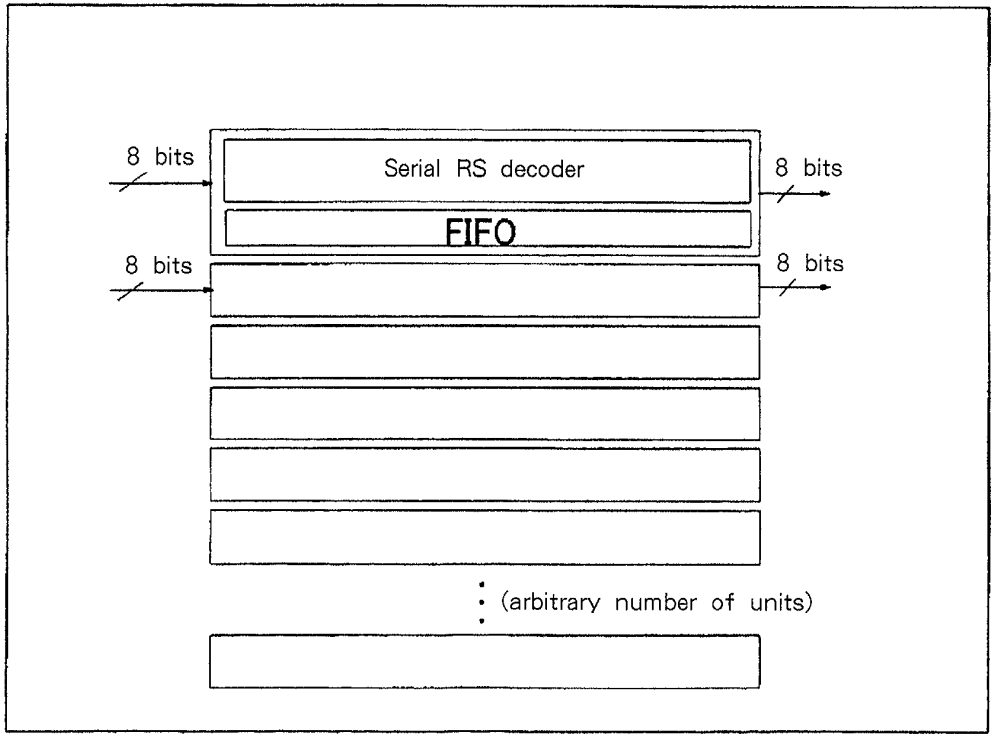


Fig. 2
PRIOR ART

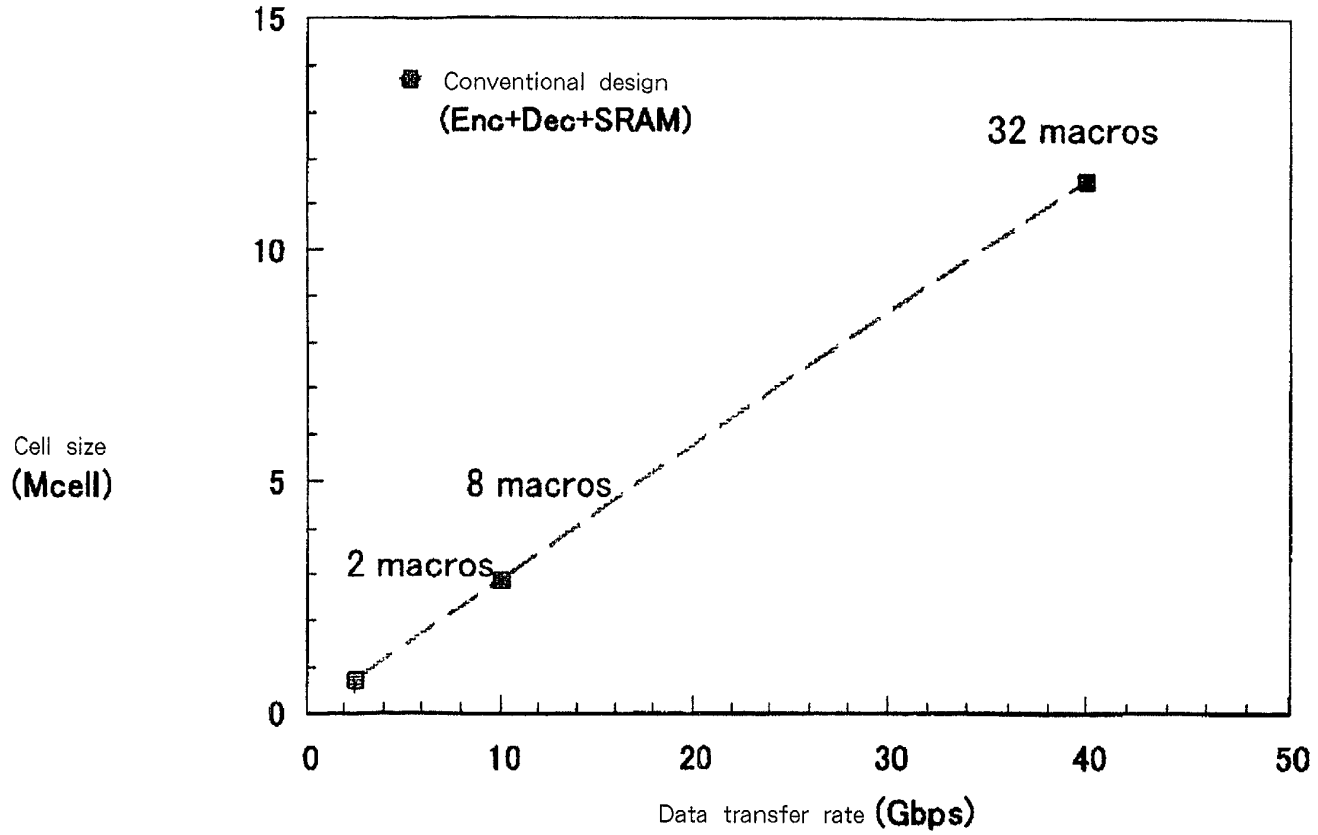


Fig. 3
PRIOR ART

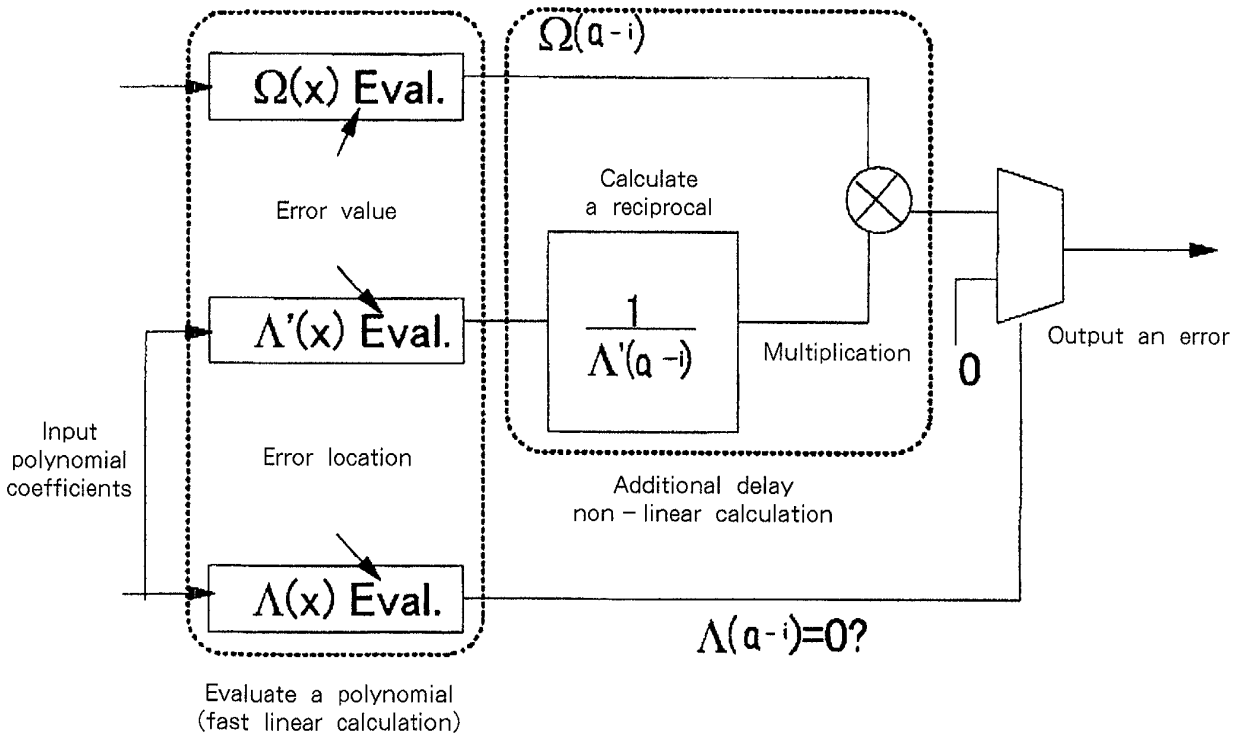


Fig. 4
PRIOR ART

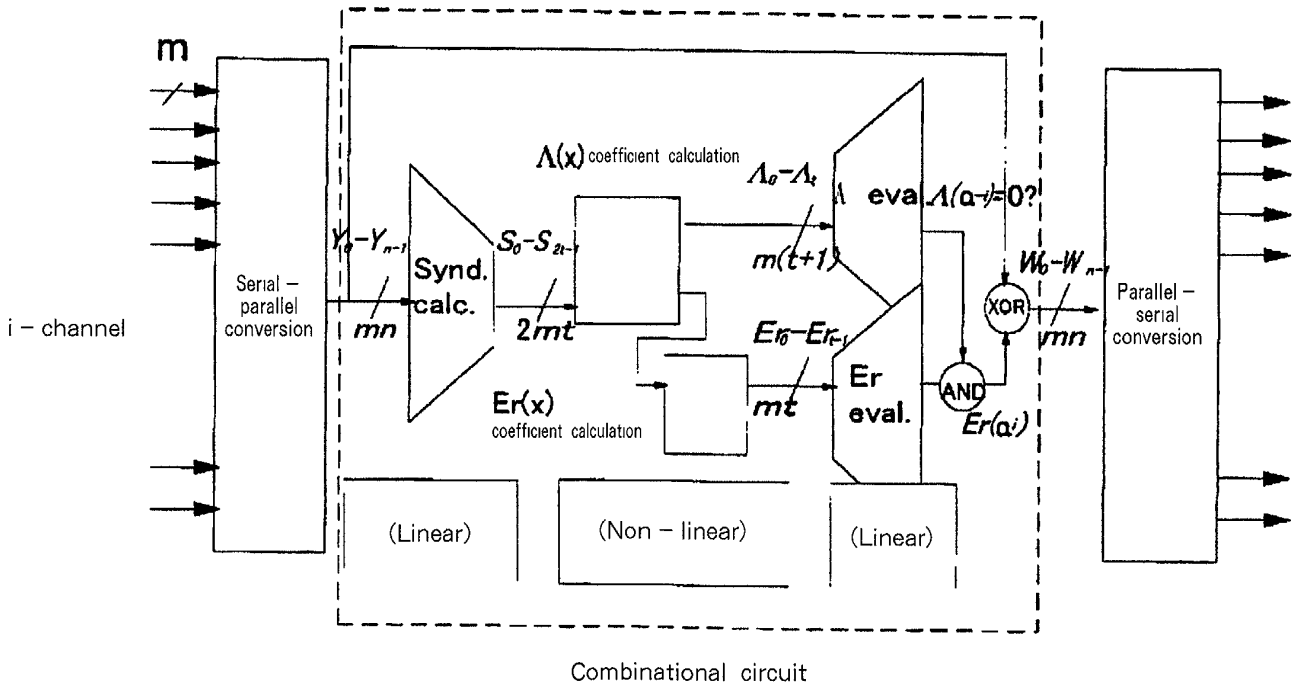


Fig. 5
PRIOR ART

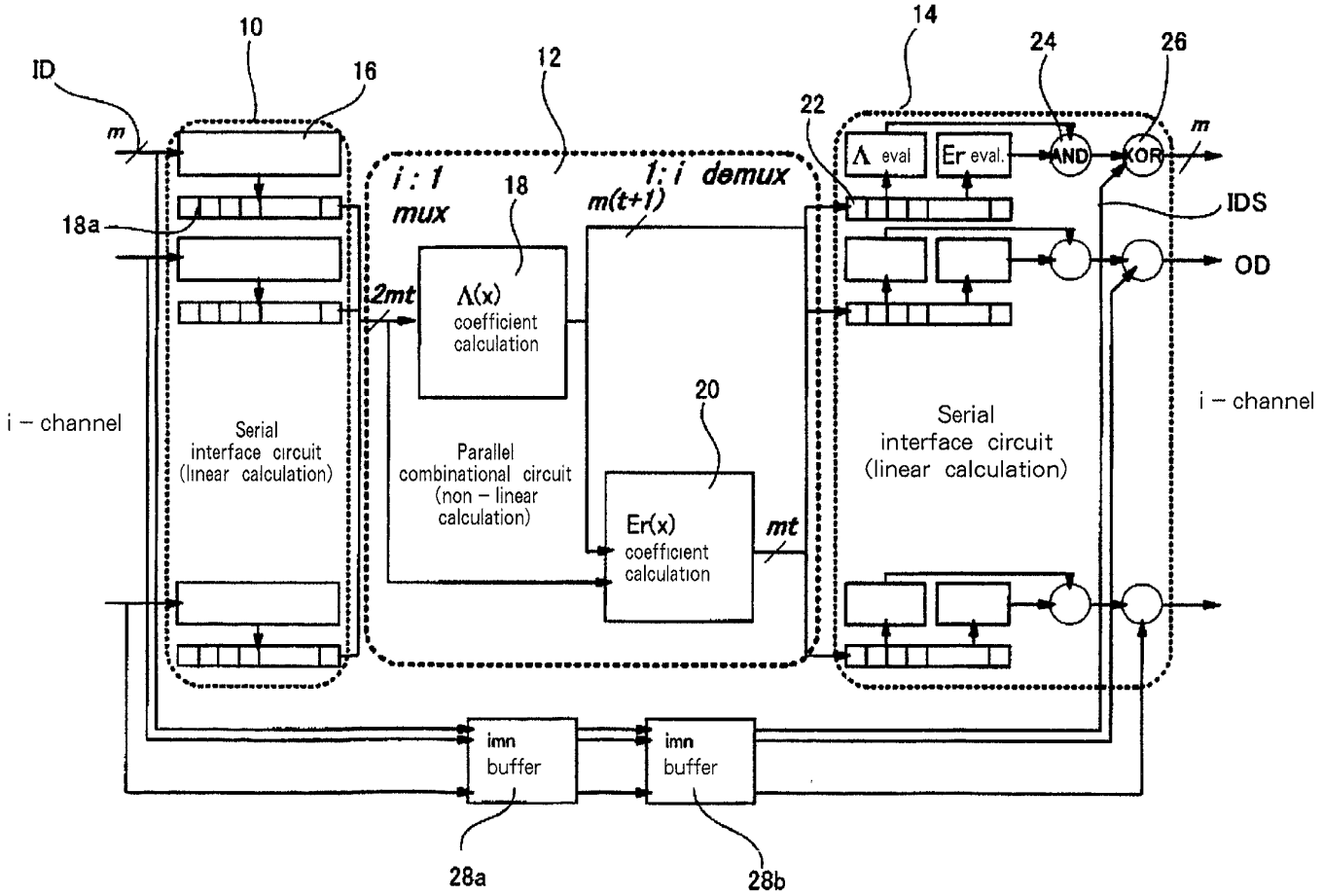


Fig. 6

PRIOR ART

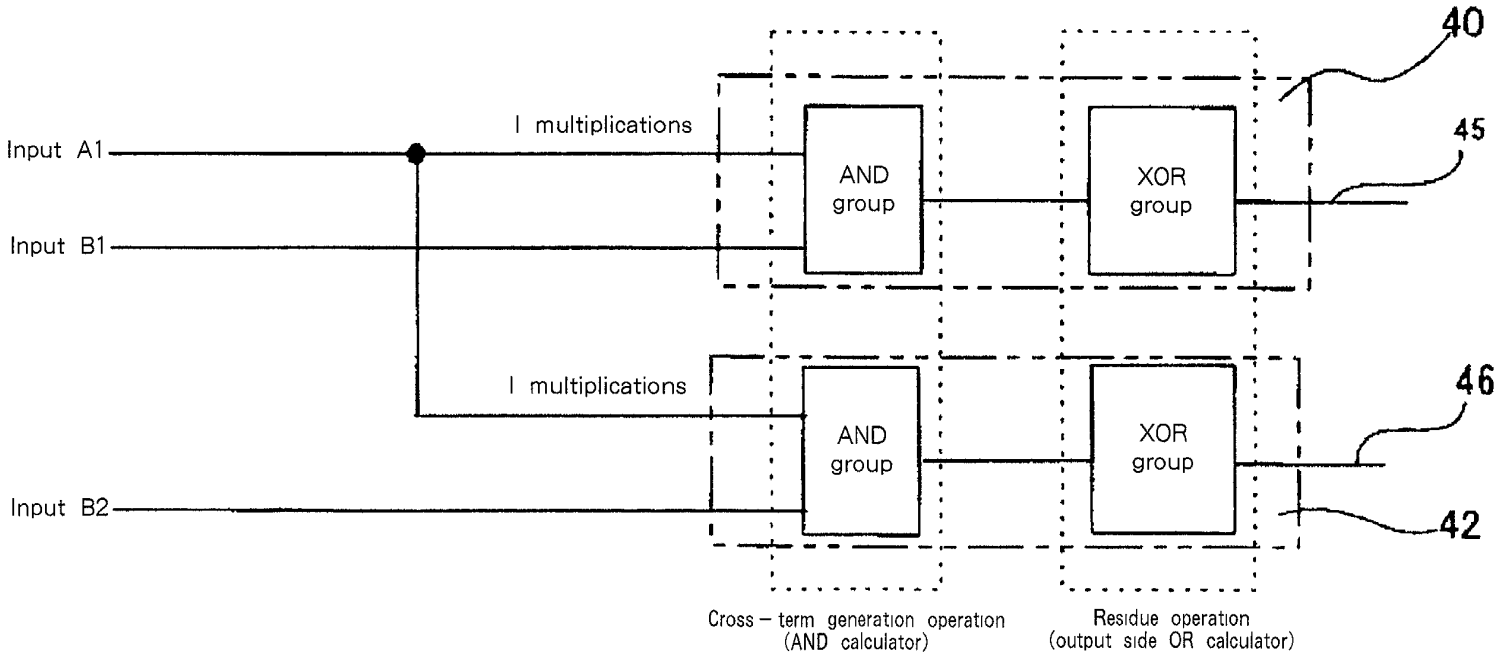


Fig. 7

PRIOR ART

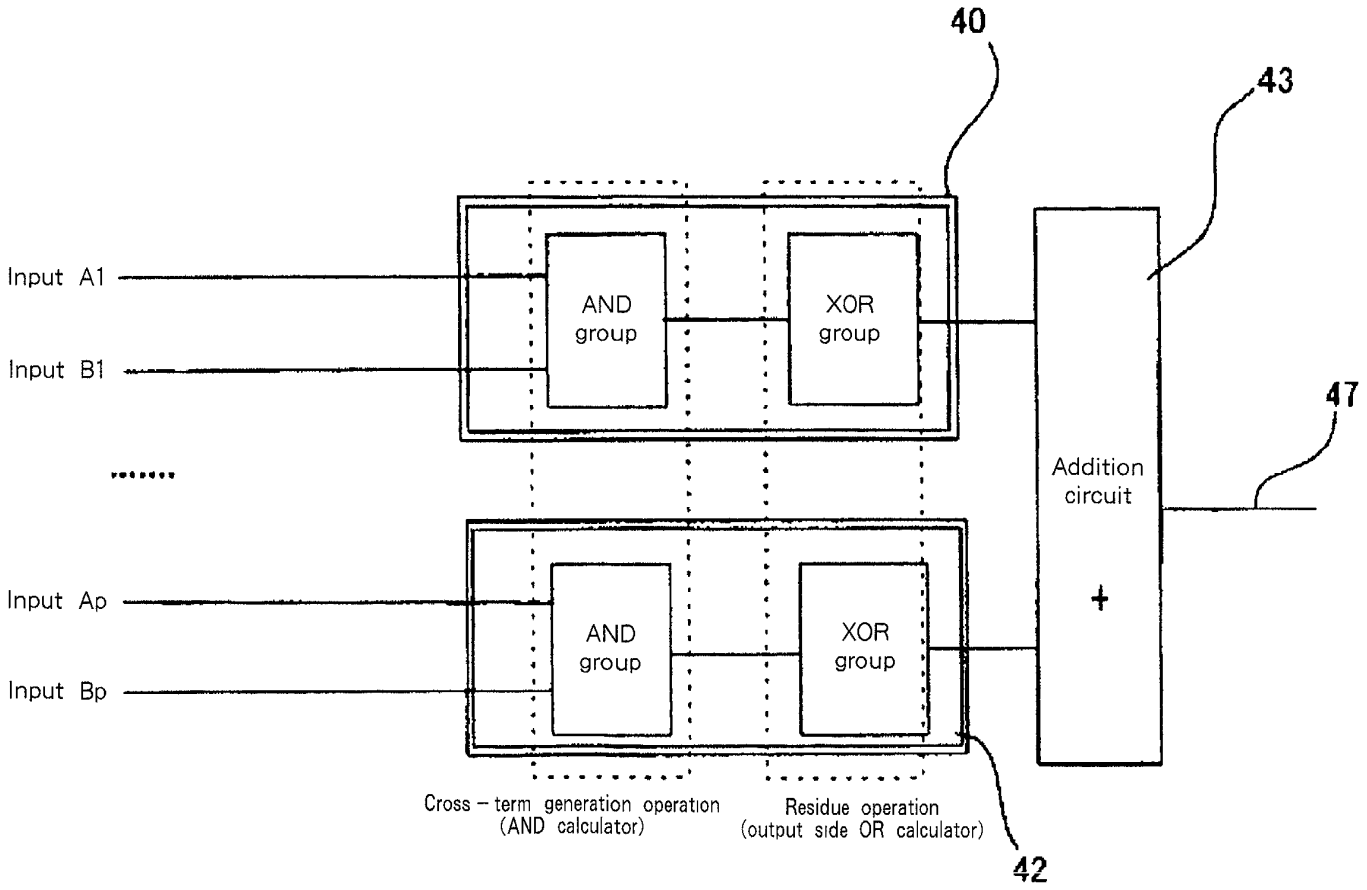


Fig. 8

PRIOR ART

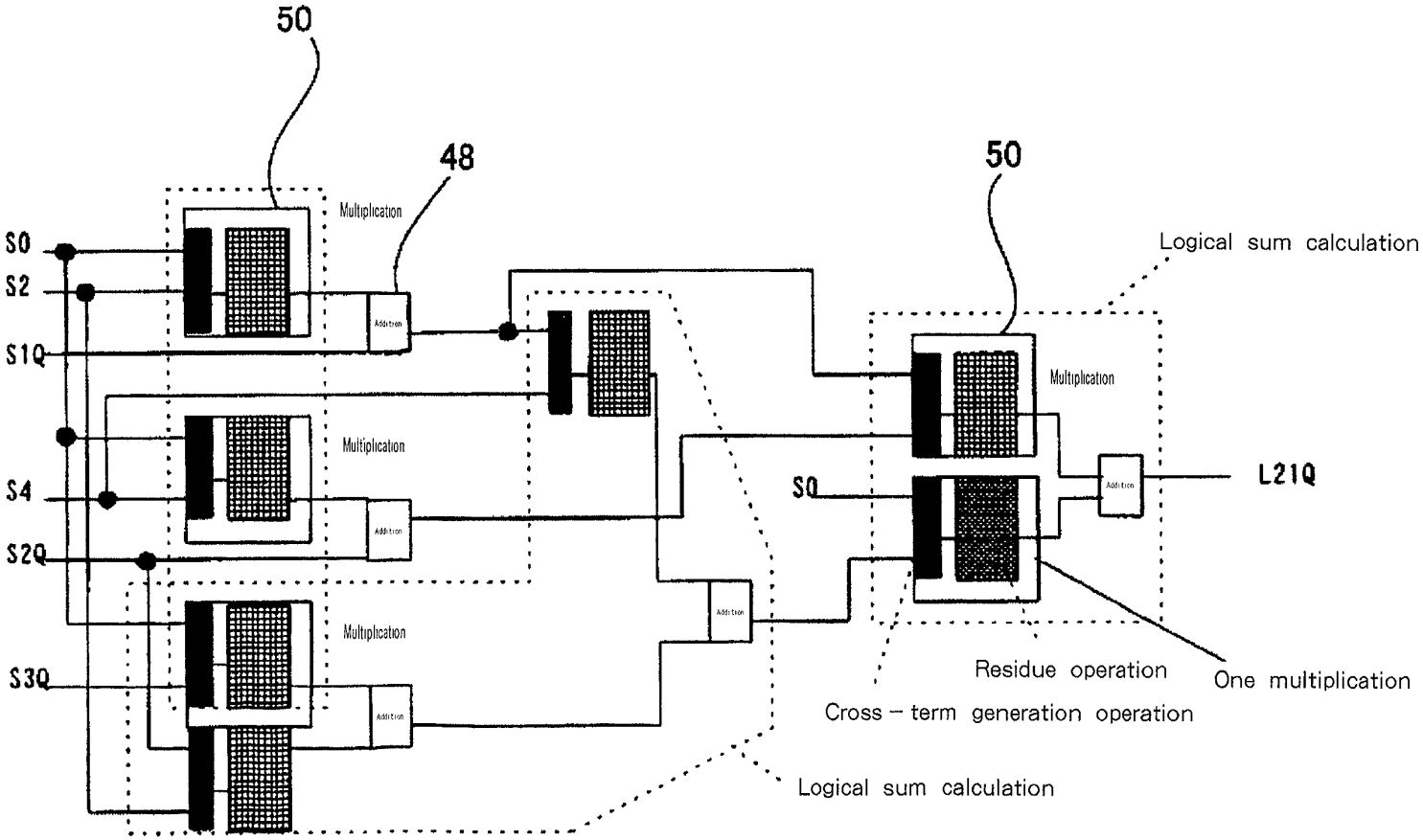
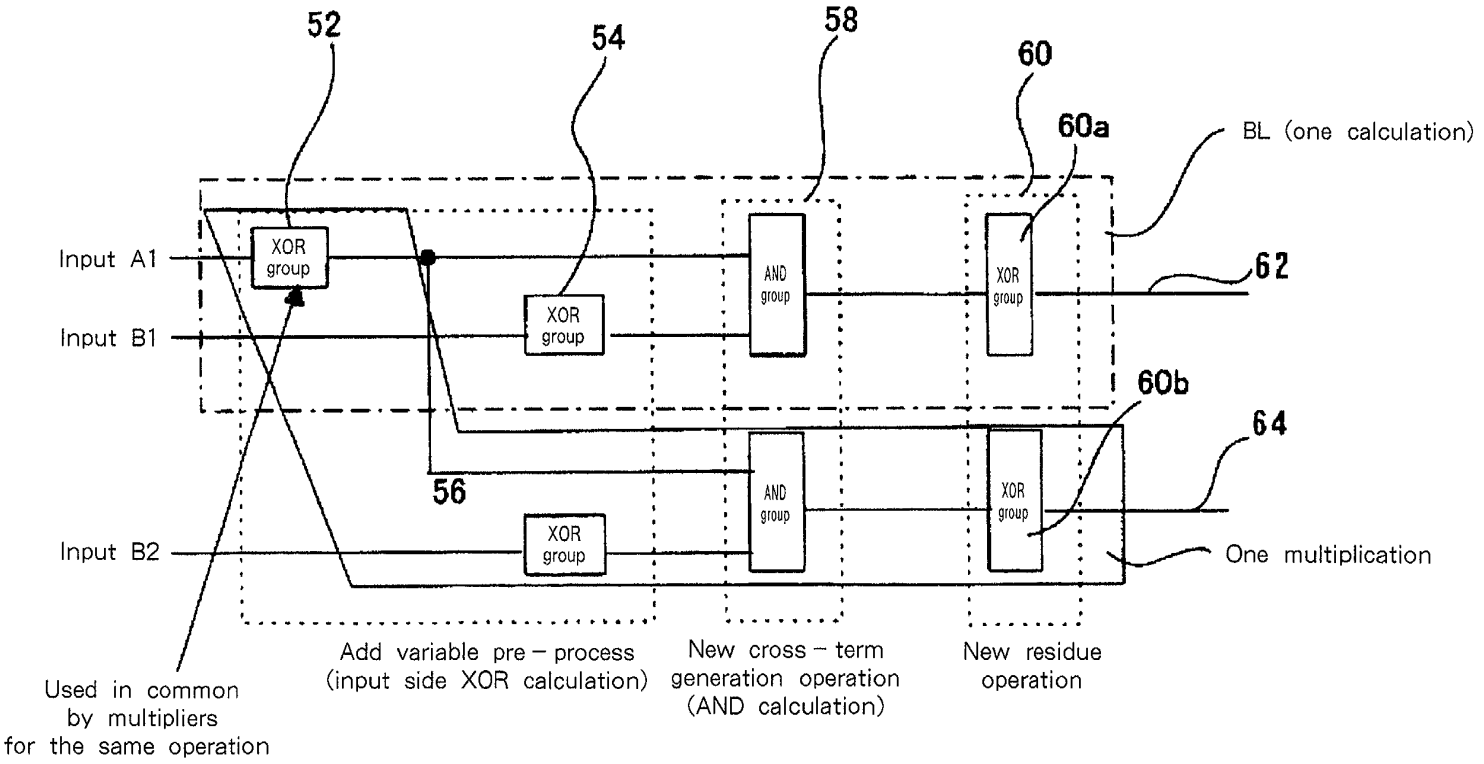


Fig. 9

PRIOR ART



(other XOR group that is not used in common and may differ for each multiplication)

Fig. 10

PRIOR ART

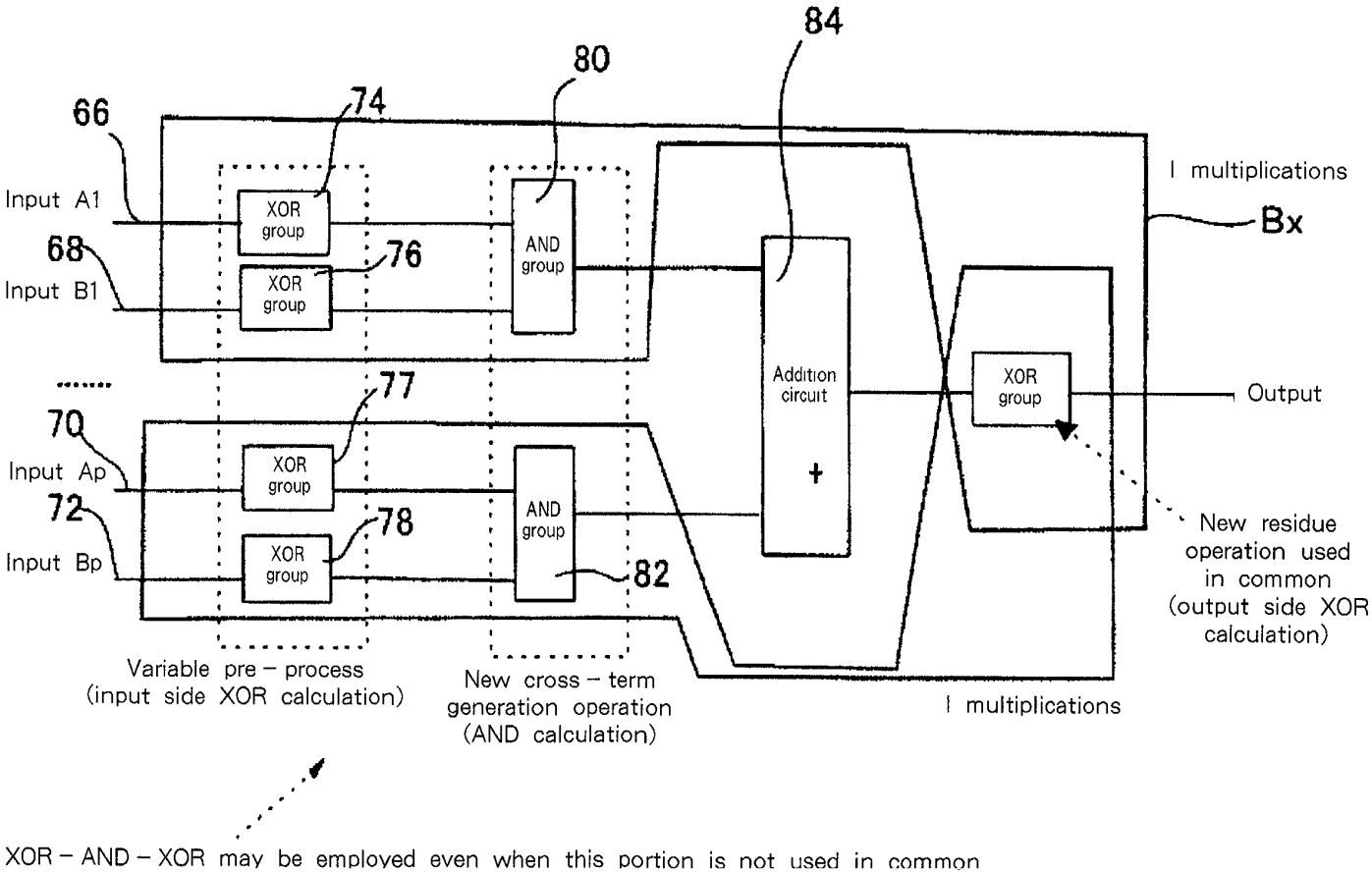


Fig. 11

PRIOR ART

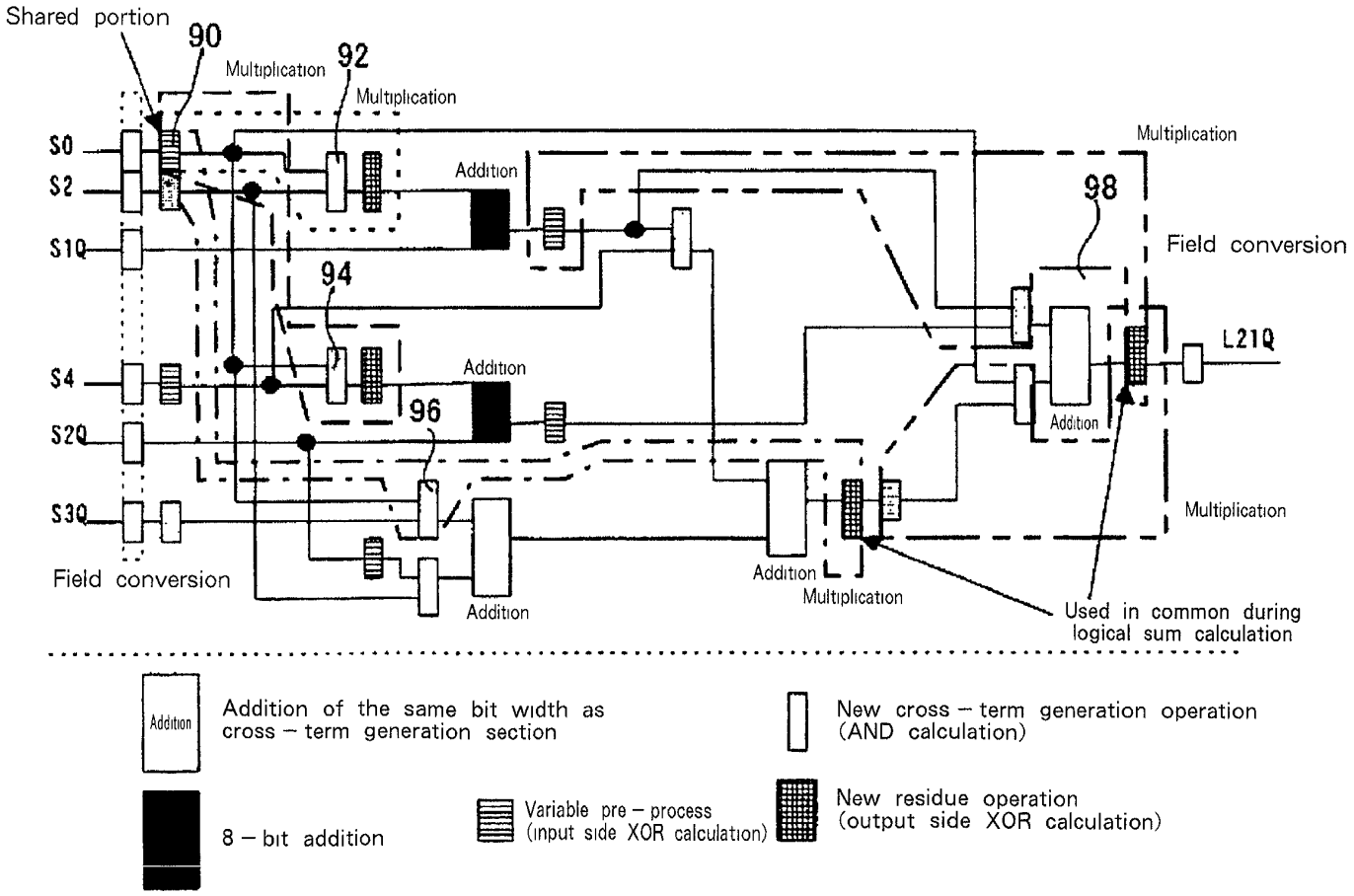


Fig. 12

PRIOR ART

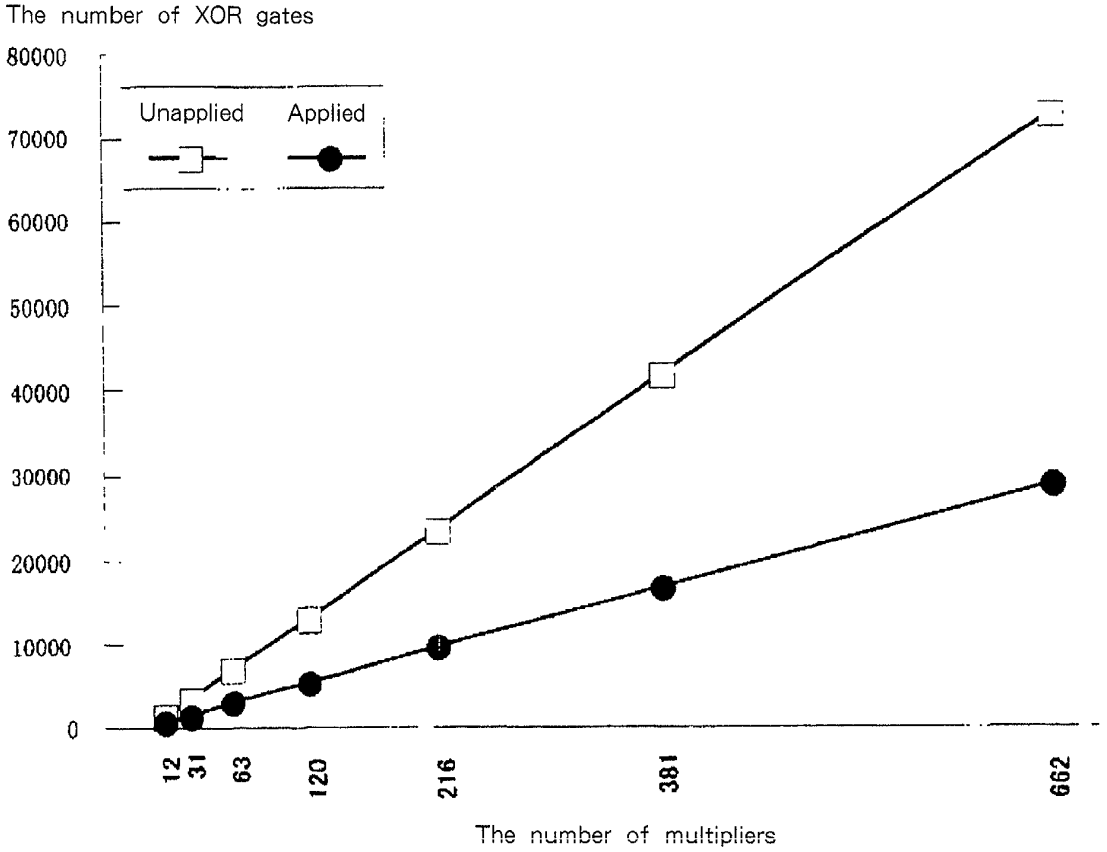


Fig. 13

PRIOR ART

$$\tilde{\Lambda}_1^{(1)} = S_1$$

$$\tilde{\Lambda}_0^{(1)} = S_0$$

Case where l = 2

$$\tilde{\Lambda}_2^{(2)} = \tilde{\Lambda}_1^{(1)} S_3 + S_2^2$$

$$\tilde{\Lambda}_1^{(2)} = \tilde{\Lambda}_0^{(1)} S_3 + \tilde{\Lambda}_1^{(1)} S_2$$

$$\tilde{\Lambda}_0^{(2)} = \tilde{\Lambda}_0^{(1)} S_2 + \tilde{\Lambda}_1^{(1)} S_1$$

Case where l = 3

$$\tilde{\Lambda}_3^{(3)} = \tilde{\Lambda}_2^{(2)} S_5 + S_1 S_4^2 + S_3^3$$

$$\tilde{\Lambda}_2^{(3)} = \tilde{\Lambda}_1^{(2)} S_5 + \tilde{\Lambda}_2^{(2)} S_4 + S_0 S_4^2 + S_2 S_3^2$$

$$\tilde{\Lambda}_1^{(3)} = \tilde{\Lambda}_0^{(2)} S_5 + \tilde{\Lambda}_1^{(2)} S_4 + \tilde{\Lambda}_2^{(2)} S_3$$

$$\tilde{\Lambda}_0^{(3)} = \tilde{\Lambda}_0^{(2)} S_4 + \tilde{\Lambda}_1^{(2)} S_3 + \tilde{\Lambda}_2^{(2)} S_2$$

Case where l = 4

$$\tilde{\Lambda}_4^{(4)} = \tilde{\Lambda}_3^{(3)} S_7 + \tilde{\Lambda}_2^{(2)} S_6^2 + S_4^4 + S_3 S_4^2 S_5 + S_3^2 S_5^2 + S_1 S_5^3$$

$$\tilde{\Lambda}_3^{(4)} = \tilde{\Lambda}_2^{(3)} S_7 + \tilde{\Lambda}_3^{(3)} S_6 + \tilde{\Lambda}_1^{(2)} S_6^2 + S_3 S_4^3 + S_2 S_4^2 S_5 + S_1 S_4 S_5^2 + S_0 S_5^3$$

$$\tilde{\Lambda}_2^{(4)} = \tilde{\Lambda}_1^{(3)} S_7 + \tilde{\Lambda}_2^{(3)} S_6 + \tilde{\Lambda}_3^{(3)} S_5 + \tilde{\Lambda}_0^{(2)} S_6^2 + S_3^2 S_4^2 + S_2 S_4^3 + S_2^2 S_5^2 + S_0 S_4 S_5^2$$

$$\tilde{\Lambda}_1^{(4)} = \tilde{\Lambda}_0^{(3)} S_7 + \tilde{\Lambda}_1^{(3)} S_6 + \tilde{\Lambda}_2^{(3)} S_5 + \tilde{\Lambda}_3^{(3)} S_4$$

$$\tilde{\Lambda}_0^{(4)} = \tilde{\Lambda}_0^{(3)} S_6 + \tilde{\Lambda}_1^{(3)} S_5 + \tilde{\Lambda}_2^{(3)} S_4 + \tilde{\Lambda}_3^{(3)} S_3.$$

Fig. 14

PRIOR ART

$$\Lambda_i^{(l)} = \frac{\tilde{\Lambda}_i^{(l)}}{\tilde{\Lambda}_0^{(l)}}, \quad i = 1, \cdots, l$$

$$\tilde{\Lambda}_0^{(l)} = \begin{vmatrix} S_0 & \cdots & S_{l-1} \\ \vdots & \ddots & \vdots \\ S_{l-1} & \cdots & S_{2l-2} \end{vmatrix},$$

$$\tilde{\Lambda}_i^{(l)} = \begin{vmatrix} S_0 & \cdots & S_{l-1} \\ \vdots & \ddots & \vdots \\ S_{l-i-1} & \cdots & S_{2l-i-2} \\ S_{l-i+1} & \cdots & S_{2l-i} \\ \vdots & \ddots & \vdots \\ S_l & \cdots & S_{2l-1} \end{vmatrix}, \quad i = 1, \cdots, l-1$$

$$\tilde{\Lambda}_l^{(l)} = \begin{vmatrix} S_1 & \cdots & S_l \\ \vdots & \ddots & \vdots \\ S_l & \cdots & S_{2l-1} \end{vmatrix}.$$

Fig. 15

PRIOR ART

$$\Gamma_0^{(l+1)} = \begin{vmatrix} S_0 & S_1 & \cdots & S_{l-1} \\ S_1 & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ S_{l-1} & \cdots & \cdots & S_{2l-2} \end{vmatrix},$$

$$\Gamma_i^{(l+1)} = \begin{vmatrix} S_0 & \cdots & S_{l-1-i} & S_{l+1-i} & \cdots & S_l \\ \vdots & & \vdots & \vdots & & \vdots \\ S_{l-1-i} & \cdots & S_{2(l-1-i)} & S_{2(l-i)} & \cdots & S_{2l-1-i} \\ S_{l+1-i} & \cdots & S_{2(l-i)} & S_{2(l+1-i)} & \cdots & S_{2l+1-i} \\ \vdots & & \vdots & \vdots & & \vdots \\ S_l & \cdots & S_{2l-1-i} & S_{2l+1-i} & \cdots & S_{2l} \end{vmatrix} \qquad i = 1, \cdots, l-1$$

$$\Gamma_l^{(l+1)} = \begin{vmatrix} S_2 & \cdots & \cdots & S_{l+1} \\ \vdots & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ S_{l+1} & \cdots & \cdots & S_{2l} \end{vmatrix}.$$

Fig. 16

PRIOR ART

$$\Gamma_0^{(1)} = 1$$

$$\Gamma_0^{(2)} = S_0$$
$$\Gamma_1^{(2)} = S_2$$

$$\Gamma_0^{(3)} = S_0 S_2 + S_1^2$$
$$\Gamma_1^{(3)} = S_0 S_4 + S_2^2$$
$$\Gamma_2^{(3)} = S_2 S_4 + S_3^2$$

$$\Gamma_0^{(4)} = \Gamma_0^{(3)} S_4 + S_0 S_3^2 + S_2^3$$
$$\Gamma_1^{(4)} = \Gamma_0^{(3)} S_6 + S_0 S_4^2 + S_2 S_3^2$$
$$\Gamma_2^{(4)} = \Gamma_1^{(3)} S_6 + S_0 S_5^2 + S_4 S_3^2$$
$$\Gamma_3^{(4)} = \Gamma_2^{(3)} S_6 + S_2 S_5^2 + S_4 S_4^2$$

$$\Gamma_0^{(5)} = \Gamma_0^{(4)} S_6 + \Gamma_0^{(3)} S_5^2 + \Gamma_1^{(3)} S_4^2 + \Gamma_2^{(3)} S_3^2$$
$$\Gamma_1^{(5)} = \Gamma_0^{(4)} S_8 + \Gamma_0^{(3)} S_6^2 + \Gamma_1^{(3)} S_5^2 + \Gamma_2^{(3)} S_4^2$$
$$\det 03 = S_0 S_6 + S_3^2$$
$$\det 24 = S_2 S_6 + S_4^2$$
$$\Gamma_2^{(5)} = \Gamma_1^{(4)} S_8 + \Gamma_0^{(3)} S_7^2 + \det 03 \cdot S_5^2 + \det 24 \cdot S_4^2$$
$$\det 45 = S_4 S_6 + S_5^2$$
$$\Gamma_3^{(5)} = \Gamma_2^{(4)} S_8 + \Gamma_1^{(3)} S_7^2 + \det 03 \cdot S_6^2 + \det 45 \cdot S_4^2$$
$$\Gamma_4^{(5)} = \Gamma_3^{(4)} S_8 + \Gamma_2^{(3)} S_7^2 + \det 24 \cdot S_6^2 + \det 45 \cdot S_5^2$$
$$\Gamma_0^{(6)} = \Gamma_0^{(5)} S_8 + \Gamma_0^{(4)} S_7^2 + \Gamma_1^{(4)} S_6^2 + \Gamma_2^{(4)} S_5^2 + \Gamma_3^{(4)} S_4^2.$$

Fig. 17

PRIOR ART

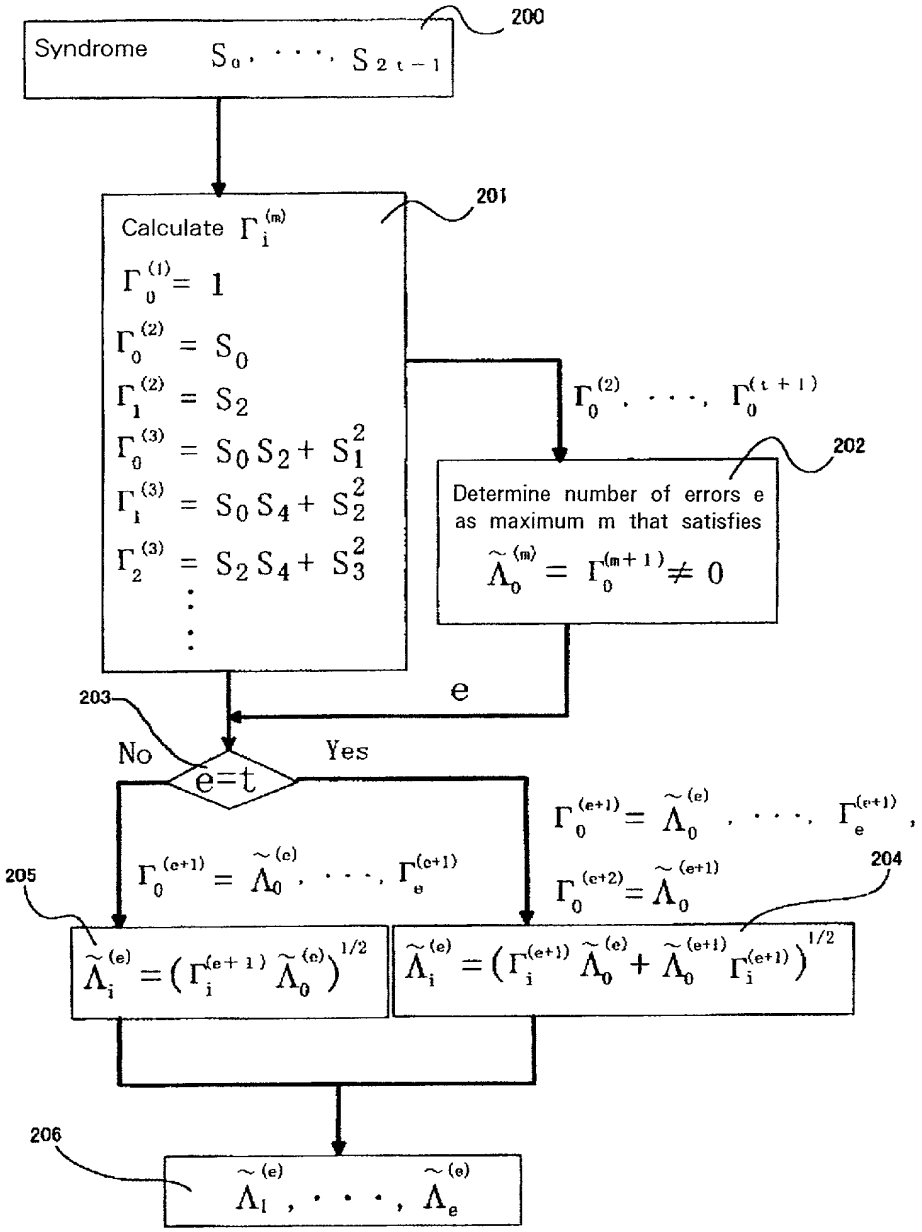


Fig. 18

PRIOR ART

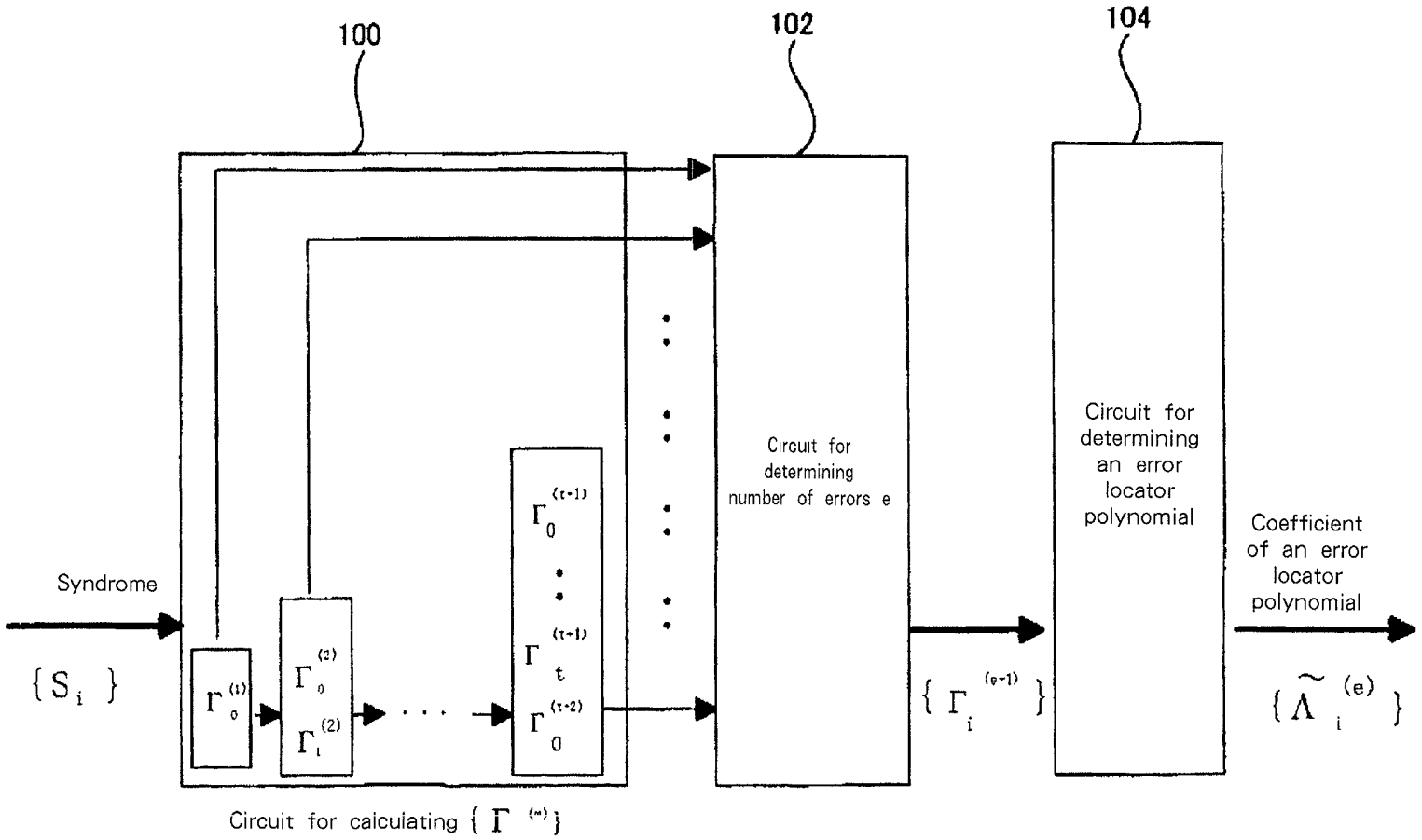


Fig. 19

PRIOR ART

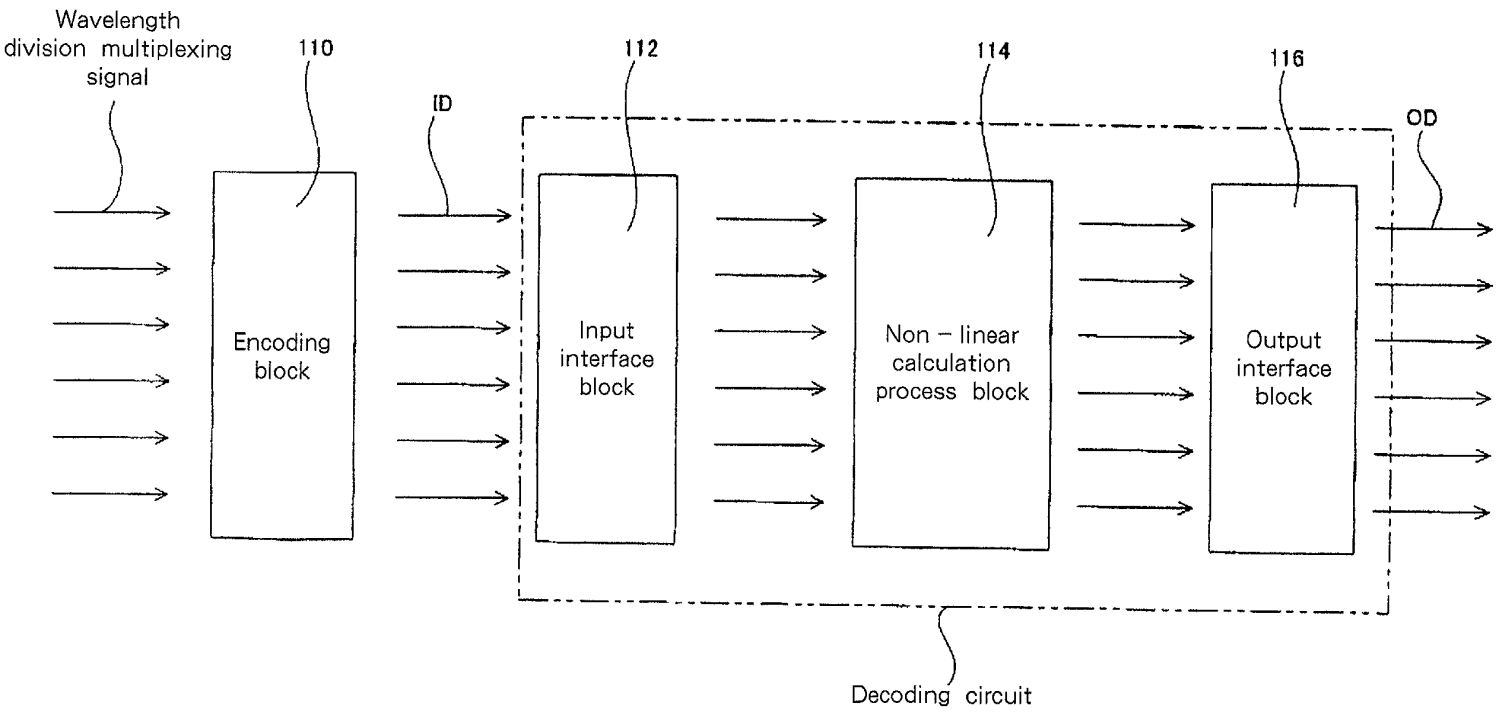


Fig. 20

PRIOR ART